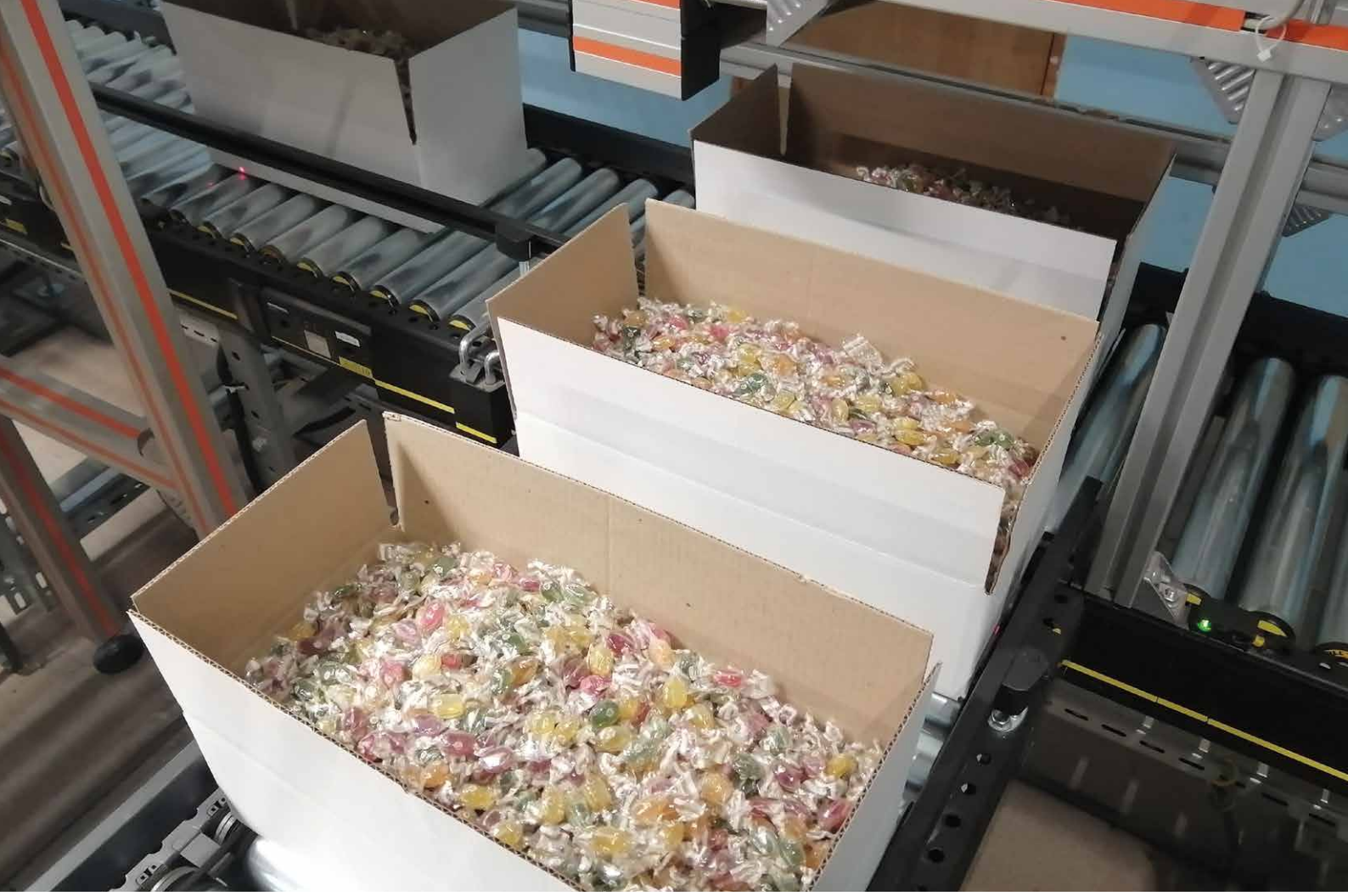

АПРОТЕХ

Производственные линии «Вознесенского пищевого комбината» под защитой «Лаборатории Касперского»

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Вознесенский пищевой комбинат

Частная производственная компания ООО «Вознесенский пищевой комбинат» (ВПК, Заказчик) основана в 1996 году. Основной профиль деятельности компании – производство и продажа кондитерских изделий. Компания специализируется на производстве таких видов кондитерских изделий, как молочные конфеты, желейный мармелад, мини-карамель, халва.

Производство ВПК сертифицировано в соответствии с требованиями международных сертификатов качества и безопасности продуктов питания. Важнейшей задачей предприятия является поддержание высокого качества продукции, поэтому на ВПК внедрена система управления качеством и установлено все необходимое оборудование для контроля качества продукции и поступающего сырья, а также соответствующих исследований.

Пищевая промышленность

- Основана в 1996 году
- Московская область, Россия
- Общий объем производства продукции составляет более 14 тысяч тонн в год

http://www.vpkbox.ru/

Задача

ВПК ориентируется на надежных поставщиков индустриальных решений для пищевой промышленности (Siemens, B&R, др.). Вопросы кибербезопасности находятся в фокусе учредителей компании и IT-команды. Приоритизация задач привела к реализации коммерческого проекта защиты финансового и управленческого контуров в начале 2019 года с использованием решений «Лаборатории Касперского».

Использование мультивендорных решений в контуре АСУ ТП, а также органический рост производственных мощностей, предполагающий наращивание технологических установок и новых подключений, предъявляют особые требования к промышленной кибербезопасности для обеспечения устойчивого роста бизнеса компании. В рамках стартовавшей кампании по расширению производственной линии ВПК была достигнута договоренность пилотирования полноценного решения Kaspersky Industrial CyberSecurity (KICS) на реальном ограниченном сегменте технологического процесса.

В рамках данного проекта отрабатывались вопросы защиты ключевых активов компании от различного рода массовых кибератак (Ransomware (вымогатели-шифровальщики), вирусы и «эксплойты», ориентированные на старые версии операционных систем и уязвимости контроллеров) и вопросы контроля доступа к критически важным ресурсам ВПК со стороны своих инженеров и специалистов, осуществляющих запуск (иногда удаленно), настройку и эксплуатацию промышленного оборудования.

В рамках пилотного проекта одной из задач было определение сегмента АСУ ТП для развертывания KICS. С одной стороны, требовалось выбрать наиболее типичные элементы для мониторинга, а с другой – минимизировать усилия по развертыванию и настройке решения. Подготовительная работа вместе с IT-командой заказчика и специалистами бизнес-партнера НПО «Адаптивные промышленные технологии» (НПО «АПРОТЕХ») позволила спроектировать и развернуть решение за два дня.

Одним из дополнительных требований со стороны Заказчика была необходимость обеспечения простого и понятного интерфейса по обнаружению и интерпретации событий, представляющих интерес в контексте промышленной кибербезопасности. Поэтому в пилот были включены сессии по передаче знаний и навыков «обучения» основной компоненты решения правилам создания «белых списков» разрешенных элементов и событий.

«Важно отметить, что тема промышленной кибербезопасности в России актуальна не только для критических инфраструктур, но и для легкой и пищевой промышленности с высоким уровнем автоматизации. Данный проект отлично демонстрирует рост зрелости рынка и стремление к безопасному и качественному производству.»

Алексей Петухов,
менеджер по развитию бизнеса
Kaspersky Industrial CyberSecurity,
«Лаборатория Касперского»

Решение

Начальная стадия реализации проекта предусматривала разработку архитектуры решения и выбор пилотного сегмента. По согласованию с Заказчиком данная архитектура затрагивала основные производственные домены (производство, фасовка и склад). Компоненты решения KICS были подобраны в составе

и количестве, которые соответствуют используемым элементам АСУ ТП на уровне SCADA-систем, контроллеров и вспомогательных программных решений.

KICS for Nodes обеспечивает киберзащиту серверов и рабочих станций в АСУ ТП, при этом потребляет меньше системных ресурсов и поддерживает возможность установки и обновления без перезагрузки. Продукт сертифицирован с наиболее распространенными программными и аппаратными компонентами промышленных систем автоматизации.

KICS for Networks создан для мониторинга и защиты промышленных сетей. Продукт не оказывает влияния на целостность производственных процессов, так как анализ трафика происходит в пассивном режиме. Широкие возможности контроля целостности сети и система обнаружения вторжений позволяют своевременно уведомить оператора об отклонениях состояния производственного процесса.

«В рамках проекта с «Вознесенским Пищевым Комбинатом» мы на практике убедились, что вопросы кибербезопасности, как части новых типов риска, находятся в фокусе владельцев предприятия. Даже новые сценарии использования промышленных данных оцениваются исходя из их ценности для бизнеса, безопасности и стоимости.»

Андрей Суворов,
генеральный директор,
НПО «Адаптивные Промышленные Технологии (АПРОТЕХ)

Результаты

Практика комплексного решения задач киберзащиты промышленного сегмента, которую в данном проекте продемонстрировала объединенная команда «Лаборатории Касперского» и НПО «АПРОТЕХ», соответствовала ожиданиям ВПК и свела к нулю риски влияния процесса развертывания решения на производство. Результаты, полученные в рамках проекта, показали эффективность системы в части обнаружения инцидентов и снижения внеплановых простоев.

В настоящее время система функционирует в пилотном режиме, обеспечивающем как обучение новым правилам по работе с разрешенными элементами и событиями, так и полноценный мониторинг промышленного трафика и событий на уровне операторских машин. Решение о переводе в коммерческое использование будет сделано по результатам этой работы.

«Кооперация с коллегами из «Лаборатории Касперского» и АПРОТЕХа позволила мне не только приоритизировать активы компании для повышения их киберустойчивости, но и наметить первые планы использования доверенных промышленных данных для повышения эффективности растущего производства», – Дмитрий Голдобин, генеральный директор, ООО «Вознесенский пищевой комбинат».

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity — это набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров. При этом решение не влияет на непрерывность технологических процессов.

Узнайте больше на: www.kaspersky.ru/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.ru
Cyber Threats News: www.securelist.ru

#Kaspersky
#BringontheFuture

www.kaspersky.ru

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

* Награда мирового лидера в области научных и технологических достижений на 3-й Всемирной интернет-конференции

** Специальный приз Китайской Международной Промышленной Ярмарки (CIIF) 2016